



**Stonesfield Primary School**  
Learning together to achieve our best

## **E-safety Policy**

**Approved by governors: September 2019**

**To be reviewed: September 2022**

ICT in the 21<sup>st</sup> Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, at Stonesfield Primary School we need to teach the effective use of these technologies in order to arm our young people with the skills to access life-long learning and future employment and stay safe online.

E-safety involves pupils, staff, governors and parents making best use of technology, information and training and this policy aims to create and maintain a safe technological environment for all pupils, staff and visitors.

*"As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal."*

From: Safeguarding Children in a Digital World. BECTA 2006

Schools have a statutory duty to keep children safe and this policy should be read alongside:

- Keeping Children Safe in Education (part one). [see appendix 1 for e-safety references in KCSIE]
  - Keeping Children Safe in Education Annex C: Online Safety [pages 96 – 99]
  - Staff Code of Conduct
  - DfE [Teaching online safety in schools](#)
- 
- The school's e-safety coordinator is Mr Ben Tremain
  - The e-Safety Governor is Mr Ben Whitworth
  - The e-safety Policy and its implementation shall be reviewed every 3 years.

## **Roles and Responsibilities**

### **Governors:**

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. The role of the E-Safety Governor will include:

- Annual meetings with the e-Safety Co-ordinator/Officer and as required.
- Annual monitoring of e-safety incident logs and as required.

### **Headteacher:**

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the e-Safety Co-ordinator.
- The Headteacher is responsible for ensuring that the e-safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteacher should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

### **The E-Safety Co-ordinator:**

- Takes day-to day-responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

### **E-safety in the Computing curriculum**

E-safety is taught routinely as part of the Computing curriculum in every year group as well as the annual e-safety week. The school will ensure that the needs of all pupils are met, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society.

Pupils will be taught:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Appropriate online behaviour
- How to identify online risks
- How and when to seek support

Internet use is a part of the statutory Computing curriculum and is a necessary and essential tool for staff and pupils, and so the school has a duty to provide pupils with quality internet access as part of their learning experience. However, there are inappropriate and undesirable elements that must be managed. All staff need to be aware of the range of risks associated with the use of internet technologies and their individual responsibilities relating to the safeguarding of children and themselves, in school and at home.

- The school Internet access will be designed expressly for pupil use including appropriate content filtering. The school will work in partnership with 123ICT to ensure filtering systems are as effective as possible.
- Pupils will have supervised access to online resources. Staff will preview any recommended sites before use.
- Pupils will be given clear objectives for internet use and taught what use is acceptable and what is not.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- As part of the new Computing curriculum, all year groups have digital literacy units that focus on different elements of staying safe online. These units include topics from how to use a search engine, digital footprints and cyber bullying. Pupils will learn how to seek help if they are affected by any form of online bullying.
- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law. It is illegal to copy or distribute school software or illegal software from other sources.
- If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the Headteacher, by recording the incident in an e-Safety Log, which will be stored in the Headteacher's office with other safeguarding materials. The e-Safety Log will be reviewed termly by the e-Safety Co-ordinator.
- Raw image searches are discouraged when working with pupils. If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.

### **Authorised Internet Access**

By explicitly authorising use of the school's internet access pupils, staff, governors and parents are provided with information relating to e-safety and agree to its use:

- At Stonesfield we have an Acceptable Use Agreement which is reviewed annually to safeguard and promote the welfare of staff and pupils. All staff, governors and volunteers are required to sign this agreement during induction and on an annual basis at the start of the year.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- At the start of a school year classes will agree an acceptable use contract which all children will sign prior to using any school ICT resource.
- Only authorised equipment, software and Internet access can be used within the school.

## **Email**

All staff shall have school email addresses and these are the only addresses that should be used in communications between staff regarding school matters.

Parents will not be given any teacher's email addresses and will be asked to contact teachers via the office address. If any teachers are contacted by parents on their personal email they should be redirected to the office.

## **Software security**

- A security breach, lost or stolen equipment, virus notifications, unsolicited emails and all other policy noncompliance must be reported to the headteacher.
- To minimise risk, pupils should not bring homework to school using portable memory sticks. **Work should be emailed to the office.**
- Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked').

## **Password security**

- Understanding password security is essential for pupils and pupils are reminded through the Computing curriculum
- Pupils are expected to keep their passwords secret and not to share with others, particularly their friends.
- Staff are reminded of the need for password security. Passwords should never be shared and staff must never let pupils use a staff login.

## **Social Networking**

- Social networking Internet sites (such as, MySpace, Facebook) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.
- Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered.
- Pupils at Stonesfield School are too young to use social networking sites, such as Facebook (the legal age limit is 13 year old). However, we recognise children are accessing the sites at home and provide information annually or as necessary to ensure privacy levels are high and children are aware of the risks.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

## **Reporting**

All breaches of the e-safety policy need to be recorded in the E-Safety reporting book that is kept in the general office. The details of the user, date and incident should be reported.

Incidents which may lead to child protection issues need to be passed on to the Designated Safeguarding Lead immediately – it is their responsibility to decide on appropriate action not the class teachers.

Incidents which are not child protection issues but may require intervention (e.g. cyberbullying) should be reported to the Headteacher in the same day.

Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary the local authority's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (e.g. Ceop button, trusted adult, Childline)

## **Mobile Phones and other internet enabled devices**

Many mobile phones and other devices such as smart watches have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Pupils may not bring mobile phones or any internet enabled device onto the school site.
- Staff should always use the school phone to contact parents.
- Staff, including students and visitors, are not permitted to access or use their mobile phones within the classroom. All staff, visitors and volunteers should ensure that their phones are turned off and stored safely away during the teaching day.
- Staff may use their mobile phones in the staffroom/school office.  
Staff should not use their mobile phones on school trips to take pictures of the children. On trips staff mobiles are used for emergency only.

## **Digital/Video Cameras/Photographs**

Pictures, videos and sound are not directly connected to the internet but images are easily transferred.

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.
- Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'.
- Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.

- Staff should always use a school camera or other device to capture images and should not use their personal devices.
- Photos taken by the school are subject to the GDPR 2018.

### **Published Content and the School Website**

The school website is a valuable source of information for parents and potential parents.

- Contact details on the website will be the school address, office e-mail and telephone number.
- Staff and pupils' personal information will not be published.
- The Headteacher or a nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Pupils' full names will not be used.
- Consent for photograph use will be obtained from parents when a child joins the school.
- Work will only be published with the permission of the pupil.
- Parents should only upload pictures of their own child/children onto social networking sites.
- The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

### **Information System Security**

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- E-safety will be discussed with our ICT support and those arrangements incorporated in to our agreement with them.

### **Protecting Personal Data**

Personal data will be recorded, processed, transferred and made available according to the GDPR 2018.

### **Assessing Risk**

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

### **Handling E-Safety Complaints**

- Complaints of Internet misuse will be dealt with by the Headteacher.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.

## Communication of Policy

### Pupils:

- Children will be reminded of the rules for internet access during Computing lessons
- Pupils will be informed that Internet use will be monitored.
- Pupils will be informed of the importance of being safe on social networking sites. This will be strongly reinforced across all year groups during Computing lessons and all year groups look at different areas of safety through the digital literacy lessons.

### Staff:

- All staff will be given the School e-safety Policy and its importance explained.

### Parents:

- Parents' attention will be drawn to the School e-safety Policy in newsletters and on the school website.

## Further Resources

We have found these web sites useful for e-safety advice and information.

<a href="http://www.thinkuknow.co.uk/">http://www.thinkuknow.co.uk/</a>	Set up by the Police with lots of information for parents and staff including a place to report abuse.
<a href="http://www.childnet-int.org/">http://www.childnet-int.org/</a>	Non-profit organisation working with others to "help make the Internet a great and safe place for children".

## APPENDIX 1: REFERENCES TO E-SAFETY IN KEEPING CHILDREN SAFE IN EDUCATION 2019 Part 1

### Safeguarding issues

26. All staff should have an awareness of safeguarding issues that can put children at risk of harm. Behaviours linked to issues such as drug taking, alcohol abuse, deliberately missing education and sexting (also known as youth produced sexual imagery) put children in danger.

### Peer on peer abuse

27. All staff should be aware that children can abuse other children (often referred to as peer on peer abuse). This is most likely to include, but may not be limited to:

- bullying (including cyberbullying);
- sexual harassment, such as sexual comments, remarks, jokes and online sexual harassment, which may be stand-alone or part of a broader pattern of abuse;
- sexting (also known as youth produced sexual imagery); and ...

### Safeguarding policies and procedures

56. Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare.

57. This should include:

- A staff behaviour policy (sometimes called the code of conduct) which should, amongst other things, include: acceptable use of technologies, staff/pupil relationships and communications including the use of social media.

### Online safety

87. As schools and colleges increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material. As such, governing bodies and proprietors should ensure appropriate filters and appropriate monitoring systems are in place. Additional information to support governing bodies and proprietors keep their children safe online is provided in Annex C.

### Opportunities to teach safeguarding

88. Governing bodies and proprietors should ensure that children are taught about safeguarding, including online safety. Schools should consider this as part of providing a broad and balanced curriculum.

90. Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.